AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
An iPhone touch screen cellular phone with colorful phone case in Milwaukee Police Department Inventory Number 22000955 ("Device A), and A black OnePlus touch screen phone with a black phone case in Milwaukee Police Department Inventory Inventory Number 22000955 ("Device B"), as further descried in Attachment A.

Case No. 22-854M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 3/9/22 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Nancy Joseph.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 2/23/22 @ 4:02 p.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, Wisconsin

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A
PROPERTY TO BE SEARCHED

1. The property to be searched includes, first, an iPhone touch screen cellular phone with colorful phone case belonging to Ricardo J RIVAS (W/M, 08/19/2002) on Milwaukee Police Department Inventory Number 22000955, ("Device A) and a second, A black A black OnePlus, Model:BE2025, IMEI: 990017120202045 phone with a black phone case belonging to Sunset ZABRANA-CASIANO (H/M, 12/13/1989) on Milwaukee Police Department Inventory Number 22000955 ("Device B") The Subject Devices are currently located at The Milwaukee Police Department's Property Control Section. This warrant authorizes the forensic examination of **Device A & B** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
ITEMS TO BE SEIZED

1. All records on the Subject Devices described in Attachment A that relate to violations of Title 18, United States Code, Section 922, including but not limited to:

   a. lists of customers and related identifying information.

   b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions.

   c. any information related to sources of firearms and drugs (including names, addresses, phone numbers, or any other identifying information).

   d. any information recording the schedule or travel of Ricardo J RIVAS and Sunset ZABRANA-CASIANO.

   e. Photographs and/or videos depicting possession of firearms, drugs, or money.

   f. Any evidence related to either the ownership, purchase, or possession of firearms, drugs, and money, or other assets; and

   g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Subject Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet Protocol address to communicate with using the internet including:

   a. records of Internet Protocol addresses used.

   b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

An iPhone touch screen cellular phone with colorful phone case in Milwaukee Police Department Inventory Number 22000955 ("Device A), and A black OnePlus touch screen phone with a black phone case in Milwaukee Police Department Inventory Inventory Number 22000955 ("Device B"), as further descried in Attachment A.

Case No. 22-854M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 922	Prohibited person in possession of a machine gun.

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI TFO Eulia Kazachenko
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 2/23/22

Judge's signature

City and state: Milwaukee, Wisconsin

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Eulia Kazachenko, being first duly sworn, hereby depose and state as follows:

BACKGROUND

1. I have been employed with the Milwaukee Police Department as a full time sworn police officer since June 2014. I am currently assigned as a task force officer (TFO) to the Milwaukee Area Safe Streets Task Force (MASSTF) and the Federal Bureau of Investigation (FBI) Milwaukee Field Office. I was officially sworn in as a federal task force officer to work with the FBI's gang task force, which provides me with the authorization to present sworn affidavits in support of federal search warrant applications. I have received training and have experience in the area of controlled substances investigations, money laundering, financial investigations, and various methods that drug dealers use in an effort to conceal and launder the proceeds of their illicit drug trafficking enterprises. I have participated in numerous investigations involving violations of controlled substances laws to include other violations associated with the trafficking of controlled substance. I have participated in numerous drug investigations utilizing various means of investigation including but not limited to, a wire investigation, the execution of search warrants, the use of subpoenas, and the use of informants.

2. The facts in this affidavit come from my personal observations, my training and experience, my review of documents, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Based on my training, experience, and participation in drug trafficking investigations, I know and have observed the following:

a. I have learned about the manner in which individuals and organizations distribute controlled substances and/ or firearms in Wisconsin as well as in other areas of the United States.

b. I am familiar with the coded language utilized over the telephone or through text messages to discuss drug/ firearm trafficking and know that the language is often limited, guarded, and coded. I also know the various code names used to describe controlled substances and various styles of firearms.

c. I know large-scale drug and firearms traffickers often purchase and/or title their assets in fictitious names, aliases or the names of relatives, associates, or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in the names other than the drug traffickers, the drug traffickers actually own and continue to use these assets and exercise dominion and control over them.

d. I know that large-scale drug traffickers will frequently use firearms to protect their narcotics, proceeds, and persons, since such drug traffickers are reticent to involve law enforcement in their affairs.

e. I know it is common for persons involved in large-scale drug trafficking to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and/or expenditure of drug and firearms trafficking proceeds, such as currency, financial instruments, precious metals and gemstones, jewelry, books, records of real estate transactions, bank

statements and records, passbooks, money drafts, letters of credit, money orders, passbooks, letters of credit, bank drafts, cashier's checks, bank checks, safe deposit box keys and money wrappers. These items are maintained by the traffickers within residences, businesses, or other locations over which they maintain dominion and control.

f. I know it is common for drug traffickers to maintain books, records, receipts, notes ledgers, airline tickets, receipts relating to the purchase of financial instruments and/or the transfer of funds and other papers relating to the transportation, ordering, sale and distribution of firearms and controlled substances. That the aforementioned book, records, receipts, notes, ledger, etc., are maintained where the traffickers have ready access to them.

g. I know drug and firearms traffickers often use electronic equipment such as telephones, pagers, computers, telex machines, facsimile machines, currency counting machines and telephone answering machines to generate, transfer, count, record and/or store the information described in the items above, as well as conduct drug and firearm trafficking activities; and

h. I am familiar with computers, cellular telephones, pagers and their uses by drug and firearms traffickers to communicate with suppliers, customers, and fellow traffickers; That drug and firearms traffickers use these devices to record their transactions and aspects of their lifestyle related to drug and firearms dealing, whether in the form of voicemail,

email, text messages, video and audio clips, floppy disks, hard disk drives, flash drives, CD's, DVD's, optical disks, Zip disks, flash memory cards, Smart media and any data contained within such computers or cellular telephones, electronic storage media and other settings particular to such devices; I know that such devices automatically record aspects of such communications, such as lists of calls and communications, and any particularized identification assigned to those source numbers or email addresses by the owner of the devices;

i. Specifically, I know the following information can be retrieved to show evidence of use of the computer to further the drug trade and firearms trafficking activities; Computer systems and cellular telephones, including but not limited to system components, input devices, output devices, data storage devices, data transmission devices, and network devices and any data contained within such systems; and computer media and any data contained within such media and other material relating to computer systems and the internet including but not limited to, documentation, operating system software, application or access program disks, manuals, books, brochures, or notes; and computer access codes, user names, log files, configuration files, and passwords, screen names, email addresses, IP addresses and cellular / wireless telephones, SIM cards, any removable storage devices for telephones, and any data contained therein, including but not limited to stored

telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data.

4. Based upon my training and experience, I know that computer hardware and software may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime, and/or (2) the objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware and software that are (1) instrumentalities, fruits, or evidence of crime, or (2) storage devices for information about crime.

5. I have participated in several narcotics and firearms trafficking investigations that involved the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these computers, cellular phones, cameras, and other digital storage devices. On many occasions, this electronic data has provided evidence of the crimes being investigated and corroborated information already known or suspected by law enforcement.

6. This affidavit is submitted in support of an application for a search warrant seeking authorization to examine two electronic devices, described more fully in Attachment A and currently in law enforcement's possession, and the extraction from those devices of electronically stored information, described more fully in Attachment B. Law enforcement believes such electronically stored information will constitute evidence of (i) Possession of a Machine Gun (ii) and Prohibited person in possession of a firearm, in

violation of Title 18, United States Code, Sections 922.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

7. The property to be searched includes, first, an iPhone touch screen cellular phone with colorful phone case belonging to Ricardo J RIVAS (W/M, 08/19/2002) in Milwaukee Police Department Inventory Number 22000955, ("Device A), and A black OnePlus, Model:BE2025, IMEI: 990017120202045 touch screen phone with a black phone case belonging to Sunset ZABRANA-CASIANO (H/M, 12/13/1989) Milwaukee Police Department Inventory Number 22000955 ("Device B") subsequently listed as "Subject Devices". The Subject Devices are currently located at The Milwaukee Police Departments Property Control.

8. The applied-for warrant would authorize the forensic examination the Subject Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

9. The MASSTF is investigating Sunset Zabrana-Casiano, Ricardo J Rivas and other persons involved in the possession and distribution of firearms and narcotics. The investigation to date has included traditional law enforcement methods, including, but not limited to: interviews with confidential sources and sources of information; information from other law enforcement officers; and physical surveillance.

10. Affiant knows that on Sunday, January 9, 2022, at approximately 4:41PM members of the Milwaukee Police Department (MPD) Police Officer (P.O.) Andrew LANGER and P.O. Justin TORRES were patrolling in the area of South 20th Street and West Orchard Avenue, in the City and County of Milwaukee, and were in a fully marked Milwaukee Police Squad Car #398, which is equipped with working red and blue emergency lights and siren.

11. P.O. LANGER and P.O. TORRES observed a 2001 silver, Ford Ranger, pick-up truck bearing Wisconsin registration plates NX4820 traveling westbound on West Orchard St from South 20th St with a tint level below the legal threshold on the windshield of the Ranger.

12. Affiant knows that when P.O. LANGER turned the squad car around in order to affect a traffic stop, the 2001 silver Ford Ranger WI NX4820 instantly increased speed and disregarded the stop sign on South 21st St.

13. Affiant knows that officers activated their red and blue emergency lights to conduct a traffic stop for the suspected illegal tint and now failing to stop at the stop sign on West Orchard Street and South 21st Street. Officers observed the Ford Ranger quickly turned southbound and pulled into the parking space behind 2100 West Orchard Street.

14. Affiant knows that the driver (later identified as Sunset ZABRANA-CASIANO (H/M, 12/13/1989) immediately exited the driver seat, a possible indicator of him attempting to flee from police on foot; ZABRANA-CASIANO was quickly detained while Officer's investigated further.

15. Affiant knows that while P.O. LAGNER was walking ZABRANA-CASIANO away from Ford Ranger towards the squad, ZABRANA-CASIANO mentioned to P.O. LAGNER that there was a gun in the truck, and it belonged to the passenger.

16. When officers opened the driver door of the Ford Ranger, they observe a male later identified as Ricardo J. RIVAS (W/M, 08/19/2002) sitting in the front passenger seat.

17. Affiant knows that P.O. TORRES observed RIVAS glance down by his left foot on the floor towards a partially concealed handgun. When P.O. TORRES asked RIVAS if he had a gun on him, RIVAS answered that he did not while moving his left foot away from the gun.

18. Affiant knows officers recovered a black in color, Glock 40 caliber pistol bearing

serial number VWE286 (MPD Inventory 22000960) with the full auto sear attached to the handgun. This gun was recovered from the passenger side floorboard which officers believe to be within the lunge distance of both the driver and passenger. The auto sear device allows a conventional semi-automatic Glock pistol to function as a fully automatic firearm. The auto sear is classified as a machine gun under federal code 18 USC 922 and 26 USC 5845(b).

19. Affiant also knows that another gun, a black in color, Kel-Tek, 5.56 caliber, semi-automatic rifle bearing serial number NCD06 (later assigned MPD inventory# 22000963) was concealed behind the front passenger seat of the Ford Ranger; Officer's believe this gun was also in lunge distance to both occupants.

20. Affiant knows both individuals were arrested and conveyed to District Two for processing, neither occupant was legally allowed to possess a concealed firearms let alone a fully automatic firearm.

21. Affiant knows a wanted check revealed that ZAMBRANO-CASIANO is a registered sex offender from Ponce, Puerto Rico.

22. Affiant received a Criminal History Statement from Puerto Rico, Sistema De Informacion de Justicia Criminal (SIJC) conviction record which was in Spanish. The record was translated from Spanish to English which revealed that ZAMBRANO-CASIANO has been found guilty on 11/02/2010 for Sexual Assault (victim under 16years old) Case number JIS2010G0001. Affiant knows that ZAMBRANO-CASIANO's conviction is a felony, and he is therefore prohibited from a possessing a firearm.

23. Affiant knows that officers recovered a black A black OnePlus, Model:BE2025, IMEI: 990017120202045 touch screen phone which was located on the driver's seat of the Ford Rangers. ZABRANA-CASIANO requested officers bring his cellphone with him identifying this

phone as belonging to him. This phone was later was placed on Milwaukee Police Department Inventory #22000955 as item #2 which is currently in the custody of the Milwaukee Police Department.

24. Affiant known that the iPhone with the colorful phone case was located on RIVAS person, was placed on Milwaukee Police Department Inventory #22000955 as item #1 which is currently in the custody of the Milwaukee Police Department.

TECHNICAL TERMS

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may

also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic films. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it

has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and

presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

26. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online, I believe that the Subject Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

27. Based on my knowledge, training, and experience, I know that electronic devices – like the Subject Devices -- can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on such devices. This information can sometimes be recovered with forensics tools.

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a

dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Subject Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

30. *Manner of execution.* Because this warrant seeks only permission to examine Subject Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

31. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Subject Devices described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A
PROPERTY TO BE SEARCHED

1. The property to be searched includes, first, an iPhone touch screen cellular phone with colorful phone case belonging to Ricardo J RIVAS (W/M, 08/19/2002) on Milwaukee Police Department Inventory Number 22000955, ("Device A) and a second, A black A black OnePlus, Model:BE2025, IMEI: 990017120202045 phone with a black phone case belonging to Sunset ZABRANA-CASIANO (H/M, 12/13/1989) on Milwaukee Police Department Inventory Number 22000955 ("Device B") The Subject Devices are currently located at The Milwaukee Police Department's Property Control Section. This warrant authorizes the forensic examination of **Device A & B** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
ITEMS TO BE SEIZED

1. All records on the Subject Devices described in Attachment A that relate to violations of Title 18, United States Code, Section 922, including but not limited to:

   a. lists of customers and related identifying information.

   b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions.

   c. any information related to sources of firearms and drugs (including names, addresses, phone numbers, or any other identifying information).

   d. any information recording the schedule or travel of Ricardo J RIVAS and Sunset ZABRANA-CASIANO.

   e. Photographs and/or videos depicting possession of firearms, drugs, or money.

   f. Any evidence related to either the ownership, purchase, or possession of firearms, drugs, and money, or other assets; and

   g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Subject Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet Protocol address to communicate with using the internet including:

   a. records of Internet Protocol addresses used.

   b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.